PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2001-345864**
(43)Date of publication of application : **14.12.2001**

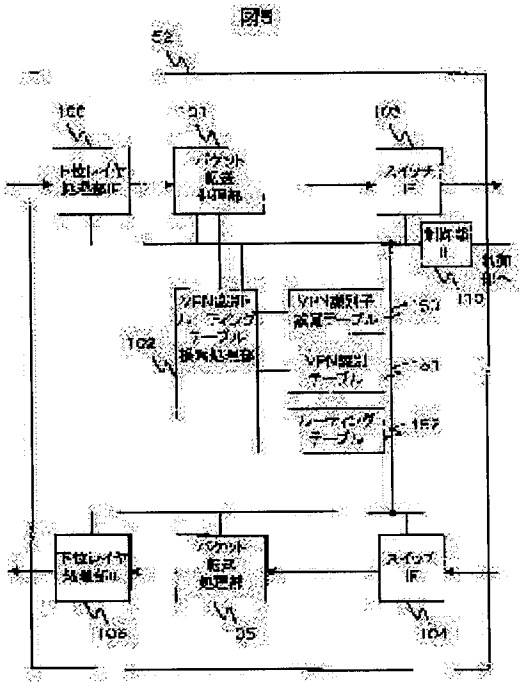
(51)Int.Cl. **H04L 12/66**
H04L 12/46
H04L 12/28
H04L 12/56

(21)Application number : **2000-170414**
(22)Date of filing : **02.06.2000**

(71)Applicant : **HITACHI LTD**
(72)Inventor : **AKAHA SHINICHI**
SAKAMOTO KENICHI
SUKAI KAZUO

(54) ROUTER DEVICE, PACKET TRANSFER CONTROL METHOD, AND SETTING METHOD FOR VPN IDENTIFICATION INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a means for identifying to which virtual private network(VPN) a received packet belongs to in an edge router which accommodates the same line, when plural VPNs are multiplexed to this line.
SOLUTION: The VPN edge router is provided with a function for identifying the VPN, while using logical channel numbers multiplexed to the same line. Thus, the VPN can be identified by using the logical channel numbers multiplexed to a physical interface. Therefore, the number of VPN to be accommodated can be increased, without having to increase the number of physical lines.



LEGAL STATUS

[Date of request for examination]	16.02.2006
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－345864
（P2001－345864A）
(43)公開日　平成13年12月14日(2001.12.14)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ 12/66		Ｈ０４Ｌ 11/20	Ｂ	５Ｋ０３０
12/46		11/00	３１０Ｃ	５Ｋ０３３
12/28		11/20	Ｇ	
12/56			１０２Ｄ	

審査請求　未請求　請求項の数23　ＯＬ　（全 18 頁）

(21)出願番号　特願2000－170414(P2000－170414)
(22)出願日　平成12年６月２日(2000.6.2)

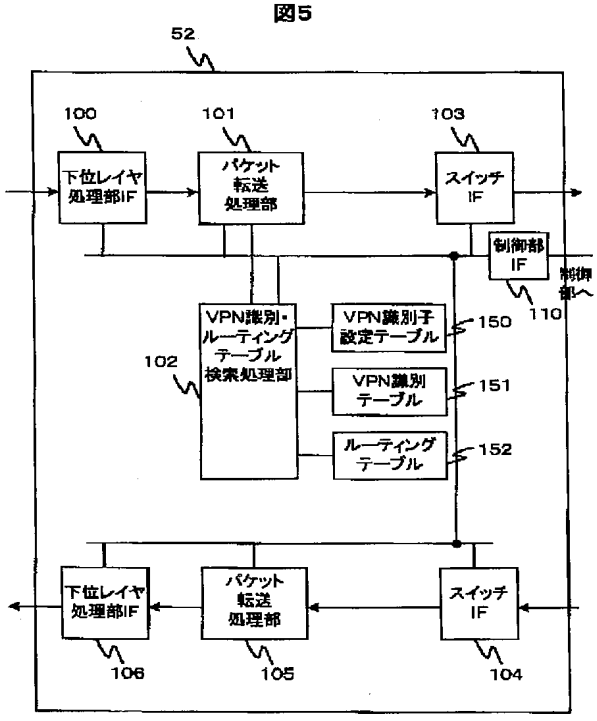
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　赤羽　真一
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(72)発明者　坂本　健一
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　ルータ装置，パケット転送制御方法及びＶＰＮ識別情報の設定方法

(57)【要約】
【課題】　同一回線に複数のＶＰＮ（Virtual Private Network）が多重される場合に、この回線を収容するエッジルータにおいて、受信したパケットが何れのＶＰＮに属するかを識別する手段を提供することである。
【解決手段】　ＶＰＮエッジルータに、同一回線に多重化されている論理的なチャネル番号を用いてＶＰＮを識別する機能を設ける。
【効果】　物理インターフェースに多重化されている論理的なチャネル番号を用いてＶＰＮを識別することができる。従って、物理回線を増やすことなく、収容するＶＰＮの数を増やすことができる。

図5



1

【特許請求の範囲】

【請求項１】複数のバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）を収容することができるルータ装置であって、

複数の論理チャネルが多重された受信回線を収容する物理インタフェースと、上記複数の論理チャネルの各論理的なチャネルに割り当てられている論理チャネル識別子と、上記複数のＶＰＮに割り当てられているＶＰＮ名との対応関係を示すテーブルを保持するメモリと、

上記複数の論理チャネルのうちの一つの論理チャネルを介して送信されたパケットを受信した際、上記論理チャネルに割り当てられている論理チャネル識別子を検索キーとして上記テーブルを検索し、上記受信パケットが上記複数のＶＰＮのうち何れのＶＰＮに属するかを判断する処理部、とを有することを特徴とするルータ装置。

【請求項２】請求項１に記載のルータ装置であって、

それぞれ、送信回線が収容される複数の物理インタフェースと、

上記複数のＶＰＮの各ＶＰＮ対応に、各ＶＰＮで使用されるパケットのアドレス情報と、上記複数の物理インタフェースを識別する情報との対応関係を示すルーティングテーブルを保持するメモリ、とを有し、

上記処理部は、上記パケットのヘッダ部に格納される宛先アドレス情報を検索キーとして上記ルーティングテーブルを検索し、上記複数の物理インタフェースのうち何れの物理インタフェースから上記受信パケットを送信するかを決定することを特徴とするルータ装置。

【請求項３】請求項２に記載のルータ装置であって、

上記ルーティングテーブルは、各ＶＰＮで使用されるパケットのアドレス情報と、パケットを出力する際に付与するヘッダ情報との関係を保持し、

上記処理部は、上記パケットのヘッダ部に格納される宛先アドレス情報を検索キーとして上記ルーティングテーブルを検索し、上記受信パケットに付与するパケットヘッダ情報を決定することを特徴とするルータ装置。

【請求項４】請求項２又は請求項３の何れかに記載のルータ装置であって、

上記テーブルと上記ルーティングテーブルとは物理的に同一のメモリ上に保持されることを特徴とするルータ装置。

【請求項５】請求項１乃至請求項４の何れかに記載のルータ装置であって、

上記受信回線は、非同期転送モード（ＡＴＭ）回線であり、上記論理チャネル識別子は、ＶＰＩ及びＶＣＩであることを特徴とするルータ装置。

【請求項６】請求項１乃至請求項４の何れかに記載のルータ装置であって、

上記受信回線は、フレームリレー回線であり、上記論理チャネル識別子は、ＤＬＣＩであることを特徴とするルータ装置。

2

【請求項７】請求項１乃至請求項４の何れかに記載のルータ装置であって、

上記受信回線は、Ｌ２ＴＰ（Layer2 Tunneling Protocol）で規定されているＬ２ＴＰヘッダでカプセル化されたパケットが送信され、上記論理チャネル識別子は、Ｌ２ＴＰカプセルヘッダ内の情報であることを特徴とするルータ装置。

【請求項８】請求項１乃至請求項４の何れかに記載のルータ装置であって、

上記受信回線は、イーサネット（登録商標）回線であり、上記論理チャネル識別子は、IEEE802.1Qで規定されるＶＬＡＮ　Ｔａｇであることを特徴とするルータ装置。

【請求項９】請求項１乃至請求項４の何れかに記載のルータ装置であって、

上記受信回線は、ＰＰＰ　Ｏｖｅｒ　Ｅｔｈｅｒｎｅｔ（登録商標）でカプセル化されたパケットが送信され、上記論理チャネル識別子は、そのカプセルヘッダ内の情報であることを特徴とするルータ装置。

【請求項１０】請求項１乃至請求項９の何れかに記載のルータ装置であって、

上記ルータ装置は、制御端末と接続することが可能であり、

上記制御端末から、上記テーブル内に保持される上記論理チャネル識別子と、上記ＶＰＮ名との対応関係を設定することができることを特徴とするルータ装置。

【請求項１１】ルータ装置であって、

第１のバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）に属する第１のローカル・エリア・ネットワーク（以下「ＬＡＮ」という。）及び第２のＶＰＮに属する第２のＬＡＮから同一のプロトコルでカプセル化されたパケットが多重されて送信される回線を収容するインタフェース部と、

上記第１の回線から受信したパケットが上記第１のＶＰＮに属するのか、上記第２のＶＰＮに属するのかを識別するための識別子を設定する手段、とを有することを特徴とするルータ装置。

【請求項１２】請求項１１に記載のルータ装置であって、

上記プロトコルは非同期転送モードプロトコルであり、上記識別子はＶＰＩ及びＶＣＩであることを特徴とするルータ装置。

【請求項１３】ルータ装置であって、

それぞれ、異なるバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）に属する複数のローカル・エリア・ネットワーク（以下「ＬＡＮ」という。）から第１のプロトコルでカプセル化されたパケットが送信される第１の回線を収容する第１のインタフェース部と、

それぞれ、異なるＶＰＮに属するＶＰＮに属する複数の

ＬＡＮから第２のプロトコルでカプセル化されたパケットが送信される第２の回線を収容する第２のインタフェース部と、

上記第１の回線から受信したパケットが何れのＶＰＮに属するのかを識別するための第１の識別子を設定する手段と、

上記第２の回線から受信したパケットが何れのＶＰＮに属するのかを識別するための第２の識別子を設定する手段とを有し、

上記第２の識別子は上記第１の識別子とは異なることを特徴とするルータ装置。

【請求項１４】請求項１３に記載のルータ装置であって、

上記第１のプロトコルは非同期転送モードプロトコルであり、上記第１の識別子はＶＰＩ及びＶＣＩであり、

上記第２のプロトコルはフレームリレーであり、上記第２の識別子はＤＬＣＩであることを特徴とするルータ装置。

【請求項１５】ルータ装置であって、

第１のバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）に属する第１のローカル・エリア・ネットワーク（以下「ＬＡＮ」という。）から第１のプロトコルでカプセル化されたパケットと、第２のＶＰＮに属する第２のＬＡＮから上記第１のプロトコルでカプセル化されたパケットととが多重されて送信される第１の回線を収容する第１のインタフェース部と、

第３のＶＰＮに属する第３のＬＡＮから第２のプロトコルでカプセル化されたパケットが送信される第２の回線と、第４のＶＰＮに属する第４のＬＡＮから上記第２のプロトコルでカプセル化されたパケットが送信される第３の回線とを収容する第２のインタフェース部と、

上記第１の回線から受信したパケットが上記第１のＶＰＮに属するのか、上記第２のＶＰＮに属するのかを識別するための第１の識別子を設定する手段と、

上記第２の回線及び上記第３の回線から受信したパケットが上記第３のＶＰＮに属するのか、上記第４のＶＰＮに属するのかを識別するための第２の識別子を設定する手段、

とを有し、

上記第２の識別子は上記第１の識別子とは異なることを特徴とするルータ装置。

【請求項１６】請求項１５に記載のルータ装置であって、

上記第１のプロトコルは非同期転送モードプロトコルであり、上記第１の識別子はＶＰＩ及びＶＣＩであり、

上記第２のプロトコルはＰＰＰ over ＳＯＮＥＴであり、上記第２の識別子は、上記第３の回線と上記第４の回線とを識別するための物理インタフェース番号であることを特徴とするルータ装置。

【請求項１７】複数のバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）を収容することができるルータ装置におけるパケット転送制御方法であって、上記ルータ装置は、複数の論理チャネルが多重された受信回線を収容し、上記複数の論理チャネルの各論理的なチャネルに割り当てられている論理チャネル識別子と、上記複数のＶＰＮに割り当てられているＶＰＮ名との対応関係を示すテーブルを有し、

上記方法は、

上記複数の論理チャネルのうちの一つの論理チャネルを介して送信されたパケットを受信し、

上記論理チャネルに割り当てられている論理チャネル識別子を検索キーとして上記テーブルを検索し、

上記受信パケットが上記複数のＶＰＮのうち何れのＶＰＮに属するかを判断する、ステップを有することを特徴とする。

【請求項１８】請求項１７に記載のパケット転送制御方法であって、

上記受信回線は、非同期転送モード（ＡＴＭ）回線であり、上記論理チャネル識別子は、ＶＰＩ及びＶＣＩであることを特徴とするパケット転送制御方法。

【請求項１９】それぞれ異なるバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）に属する複数のローカル・エリア・ネットワーク（ＬＡＮ）を収容するルータ装置におけるＶＰＮ識別情報の設定方法であって、

上記ルータ装置は、上記複数のＬＡＮの一部のＬＡＮからは第１のプロトコルでカプセル化されたパケットを受信し、上記複数のＬＡＮの他のＬＡＮからは第２のプロトコルでカプセル化されたパケットを受信し、そして、メモリを有し、上記方法は、

上記一部のＬＡＮから受信したパケットが何れのＶＰＮに属するのかを識別するための第１の識別子を上記メモリに設定し、

上記他のＬＡＮから受信したパケットが何れのＶＰＮに属するのかを識別するための第２の識別子を上記メモリに設定し、

上記第２の識別子は上記第１の識別子とは異なることを特徴とする。

【請求項２０】請求項１９に記載のＶＰＮ識別情報の設定方法であって、

上記第１の識別子と、ＶＰＮに割り当てられているＶＰＮ番号との対応関係を示す第１のテーブルを設定し、

上記第２の識別子と、ＶＰＮに割り当てられているＶＰＮ番号との対応関係を示す第２のテーブルを設定する、ステップを更に有することを特徴とするＶＰＮ識別情報の設定方法。

【請求項２１】請求項１９又は請求項２０の何れかに記載のＶＰＮ識別情報の設定方法であって、

上記第１のプロトコルは非同期転送モードプロトコルであり、上記第１の識別子はＶＰＩ及びＶＣＩであり、

上記第２のプロトコルはフレームリレーであり、上記第２の識別子はＤＬＣＩであることを特徴とするＶＰＮ識別情報の設定方法。

【請求項２２】複数のバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）を収容するルータ装置におけるパケット転送制御方法であって、

レイヤ２に相当するプロトコルによるカプセルヘッダが付与されたＩＰパケットを受信し、

上記カプセルヘッダ内の情報を用いて、上記受信したＩＰパケットが何れのＶＰＮに属するかを決定する、ステップを有することを特徴とするパケット転送制御方法。

【請求項２３】複数のバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）を収容するルータ装置であって、

レイヤ２に相当するプロトコルによるカプセルヘッダが付与されたＩＰパケットを受信するインタフェース部と、

上記カプセルヘッダ内の情報を用いて、上記受信したＩＰパケットが何れのＶＰＮに属するかを決定する手段、とを有することを特徴とするルータ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はルータ装置、そのパケット転送制御方法及びルータ装置内のルーティング情報設定方法に係り、特にインターネットにおける仮想専用網（ＶＰＮ：Virtual Private Network）を構築するルータ装置、その転送制御方法、その設定方法に関する。

【０００２】

【従来の技術】従来、異なる地域に存在する複数の企業内網をネットワークにより接続する場合、企業は企業内網を専用線で相互接続することによって、外部のネットワークから隔絶した（つまりセキュリティが確保された）ネットワークを構築していた。しかし、専用線を使用するとネットワークコストが上昇してしまうという問題があった。このため、廉価で使用できるインターネットの普及に伴い、インターネットを利用して低コストの仮想的な専用線網（以下、ＶＰＮ：Virtual Private Networkと呼ぶ）を構築する技術に対する要求が高まってきた。この技術は、ＩＰ（Internet Protocol）ネットワークが提供するＩＰあるいはＩＰの下位レイヤの機能を用いて、専用網を仮想的にインターネット上に構築するものである。この技術により、ＩＰネットワーク上でも、外部のネットワークから隔絶された安全でかつ何らかの品質保証が行えるネットワークを構築することができる。

【０００３】ＶＰＮを実現する方式としては、ＶＰＮを提供するインターネットサービスプロバイダ（以下、ＩＳＰと呼ぶ）のネットワークの入り口でカプセル化を行い、ＩＳＰのネットワーク上ではこのカプセル化したヘッダに基づき転送を行い、ネットワークの出口でカプセルヘッダをはずす方式により転送を行う方式がある。インターネットの内部ではＶＰＮ固有のカプセル化ヘッダを用いることにより、セキュリティの確保されたＶＰＮを構成することが出来る。このカプセル化の具体的なプロトコルとしては、ＩＰカプセル化、ＭＰＯＡ（Multi Protocol OverATM）、ＭＰＬＳ（Multi Protocol Label Switching）等の方式があり、２０００年５月現在、IETFなどの標準化団体で標準化が進められている。

【０００４】

【発明が解決しようとする課題】ＩＰアドレスには、グローバルＩＰアドレスと、プライベートＩＰアドレスとがある。グローバルＩＰアドレスは世界的に一意に定められるものであるのに対し、プライベートＩＰアドレスは企業が自由に定めることができるものである。企業内網では、プライベートＩＰアドレスが用いられる場合が多い。したがって、企業がＶＰＮサービスを利用する場合においても、プライベートＩＰアドレスを使用できることが望ましい。この場合、複数のＶＰＮ間で同一のＩＰアドレスが使用される可能性がある。複数のＶＰＮ間のＩＰアドレスがバッティングする場合、それぞれのＶＰＮのパケットを正しく処理するため、ＩＳＰネットワークの入り口に位置し、かつ、ＶＰＮに属するＬＡＮ（Local Area Network）を収容するルータ（以下、ＶＰＮエッジルータと呼ぶ）は、ＶＰＮ毎のルーティングテーブルを保持する必要がある。ＶＰＮエッジルータは、パケットを受信すると、そのパケットがどのＶＰＮに属するＬＡＮからのパケットかを判定する。その後、ＶＰＮエッジルータは、当該ＶＰＮ用のルーティングテーブルを検索してＩＳＰ内ネットワークでの転送先の決定、およびカプセル化を行う。ＶＰＮエッジルータはＶＰＮ毎にルーティングテーブルを保持しているので、ＶＰＮエッジルータは、異なるＶＰＮから受信した同一の宛先ＩＰアドレスを持つパケットを混同せず、正しく転送することができる。

【０００５】前記ＶＰＮを識別する方式としては、例えば「日経コミュニケーション」、１９９９年１０月１８日号、ｐ．１００、に記載されているように、ユーザ回線インターフェース単位に、ＶＰＮを一意に識別するためのＶＰＮ－ＩＤを割り当て、このＶＰＮ－ＩＤによりＶＰＮ識別を行う方式がある。すなわち、ＶＰＮの識別単位は物理インターフェース毎ということになる。この場合、物理インターフェース一つがＶＰＮ一つに対応している必要がある。

【０００６】しかし前記の方式では、企業ネットワークからＩＳＰネットワークまでが、一つの物理回線で接続されている必要がある。また、一つの企業ネットワークを複数のＶＰＮと接続させたい場合、そのＶＰＮの数だけ物理回線を用意する必要がある。さらに、ＶＰＮエッジルータは、収容するＶＰＮの数だけ物理インターフェ

ースを保持する必要がある。このため、ＶＰＮエッジルータが収容するＶＰＮの数が大きくなると、ＶＰＮエッジルータの物理インターフェース数及びルータ自体の数も大きくなるという問題がある。

【０００７】企業ネットワークからＶＰＮサービスを行うＩＳＰネットワークまでのアクセス手段として、別のＩＳＰあるいはキャリアが提供するＡＴＭ網やフレーム・リレー等を用いる場合、ＩＳＰの入り口では１つの物理インターフェース内に複数の論理的なチャネルが多重されているため、物理インターフェースでＶＰＮ識別を行うことはできないという問題もある。

【０００８】本発明の目的は、物理インターフェースに多重化されている論理的なチャネル番号を用いてＶＰＮ識別を可能にすることである。

【０００９】また、本発明の他の目的は、ルータがＬＡＮを収容する際、ＩＰの下位レイヤとして複数の異なるプロトコルを用いる場合でも、それぞれのプロトコルに対応した適切なＶＰＮ識別情報を用いてＶＰＮ識別を行うことを可能にすることである。

【００１０】

【課題を解決するための手段】前記課題を解決するため、本発明のＶＰＮエッジルータは、物理インターフェースに多重化されている論理的なチャネルを識別するためのチャネル番号を用いてＶＰＮを識別する。論理的なチャネル番号として、ＩＰの下位レイヤの情報、例えば、ＯＳＩモデルで規定されているレイヤ２に相当する情報を用いる。論理的なチャネル番号の例をいくつか挙げると、ＩＰパケットの下位レイヤがＡＴＭの場合は、ＶＰＩ、ＶＣＩ等のヘッダ情報を、下位レイヤがフレームリレーの場合はＤＬＣＩを論理的なチャネル番号として用いることができる。また、ＩＰパケットがＬ２ＴＰ（Layer2 Tunneling Protocol）で規定されているＬ２ＴＰヘッダでカプセル化されている場合には、Ｌ２ＴＰカプセルヘッダ内の情報（トンネルID、セッションID等）を論理的なチャネル番号として用いることができる。下位レイヤがイーサーネットで、IEEE802.1Qで規定されるＶＬＡＮ　Ｔａｇを用いてＶＰＮの識別が行われる場合、前記論理的なチャネル番号としてＶＬＡＮＴａｇを用いることができる。IPパケットがPPP Over Ethernetカプセル化方式で規定されているカプセル情報でカプセル化されている場合には、PPP Over Ethernetカプセル化方式で規定されているカプセル情報（セッションID等）を論理的なチャネル番号として用いることができる。

【００１１】さらに、ＶＰＮエッジルータに、ＶＰＮ識別に用いる識別子を設定するためのＶＰＮ識別子設定テーブルを設ける。この設定をＶＰＮエッジルータを管理するＩＳＰの管理者が行えるようにするため、ＶＰＮエッジルータにユーザインターフェースを設ける。ＩＰの下位レイヤがＡＴＭの場合を例に説明すると、ＶＰＮ識別を物理インターフェースで行う場合には、前記ＶＰＮ識別子設定テーブルに物理インターフェースと設定する。また、ＶＰＮ識別をＶＰＩ、ＶＣＩで行う場合には、前記ＶＰＮ識別子設定テーブルにＶＰＩ、ＶＣＩと設定する。

【００１２】ＶＰＮ識別子設定テーブルの設定単位は、物理インターフェース毎としてしてもよいし、下位レイヤとして同一のプロトコルが使用される複数の回線を収容するインターフェースカード単位でもよい。また、１つの物理インターフェース内に下位レイヤとして複数のプロトコルが多重化されている場合（例えばフレームリレーとＰＰＰが時分割多重されている回線）は、その設定単位は、物理インターフェースとＩＰの下位レイヤのプロトコルとの組合わせでもよい。

【００１３】ＩＳＰがＶＰＮを収容する際、ＩＰの下位レイヤにＡＴＭを用い、ＶＰＮ識別子としてＶＰＩ、ＶＣＩを用いる場合を例にＶＰＮエッジルータの動作を具体的に説明する。ＶＰＮエッジルータはパケットを受信すると、まず、ＶＰＮ識別子設定テーブルの設定に従い、ＶＰＮ識別子（本例の場合、ＶＰＩ、ＶＣＩと設定されている）および検索すべきＶＰＮ識別テーブルを決定する。本例の場合、ＶＰＮエッジルータは、ＶＰＩ、ＶＣＩとＶＰＮとの対応が示されているテーブルを検索することになる。ＶＰＮエッジルータは、ＶＰＩ、ＶＣＩを検索キーにしてＶＰＮ識別テーブルの検索を行い、受信したパケットがどのＶＰＮに属しているかを判定する。その判定が終了すると、ＶＰＮエッジルータは、受信したパケットが属するＶＰＮ用のルーティングテーブルを検索し、ＩＳＰネットワーク内の次の転送先を決定し、ネットワーク内でＶＰＮ識別のために使用されるカプセル化ヘッダ情報の生成を行う。ＶＰＮエッジルータは、パケットにヘッダ情報を付与し、決定した次の転送先へパケットを送出する。

【００１４】以上の説明のように、本発明では、物理インターフェースに多重化されている論理的なチャネル番号を用いてＶＰＮ識別を行うため、ＶＰＮエッジルータにＶＰＮ毎に物理インターフェースを用意する必要がない。また、一つの企業ネットワークを複数のＶＰＮと接続させたい場合、そのＶＰＮの数だけ論理的なチャネルを用意すればよく、ＶＰＮの数だけ物理的な回線を用意する必要が無い。また、企業ネットワークからＶＰＮサービスを行うＩＳＰネットワークまでのアクセス手段として、別のＩＳＰあるいはキャリアが提供するＡＴＭ網やフレーム・リレー等を用いる場合においても、論理的なチャネルでＶＰＮ識別が行われるため、ＶＰＮを実現することができる。

【００１５】さらに、本発明によれば、ＩＳＰの管理者は、ＩＰの下位レイヤのプロトコル毎にＶＰＮ識別子を選択し、そのＶＰＮ識別子をＶＰＮ識別子設定テーブルに設定することができるため、ＶＰＮを収容する際、下

位レイヤに様々のプロトコルを用いることができる。

【００１６】

【発明の実施の形態】図１は、本発明のＶＰＮエッジルータを用いて構成したＶＰＮの一実施例を説明するための図である。以下では、下位レイヤとは、ＩＰパケットをカプセル化するプロトコルを意味するものとする。また、ＩＰパケットをＩＰヘッダでカプセル化する場合にも、便宜上、このカプセルヘッダを下位レイヤのヘッダとして表記することとする。

【００１７】ＩＳＰネットワーク（５）は、ネットワークのバウンダリに位置するエッジルータ（９、１０）と、ネットワークコアに位置するコアルータ（１７）とを有する。図１では、コアルータ（１７）は一つしか示されていないが、その数はこれに限定されるものではない。ＩＳＰネットワーク（５）内部ではＭＰＬＳ（ＡＴＭによる）によりカプセル化が行われＶＰＮが実現されるものとする。上述のように、カプセル化の仕方はこれに限られない。ＩＳＰネットワーク（５）は、エッジルータ（９）を介してＬＡＮ１（１）とＬＡＮ２（２）を収容し、エッジルータ（１０）を介してＬＡＮ３（３）とＬＡＮ４（４）を収容する。ＬＡＮ１（１）とＬＡＮ３（３）は同一企業ＡのＬＡＮであり、これらのＬＡＮ間でＶＰＮを構成する。また、ＬＡＮ２（２）とＬＡＮ４（４）は同一企業ＢのＬＡＮであり、これらのＬＡＮ間でもＶＰＮを構成する。企業Ａ、企業ＢのＶＰＮをそれぞれＶＰＮＡ（７）、ＶＰＮＢ（８）と呼ぶことにする。

【００１８】ＬＡＮ１とＬＡＮ２は、ＩＳＰネットワーク（５）とは別のＩＳＰまたはキャリアが提供するＡＴＭ網（６）を介し、回線（１１）に論理的に多重化されてエッジルータ（９）に接続されている。回線（１１）とエッジルータ（９）の物理インターフェースを（１２）とする。物理インタフェースとは、ルータと回線との接続点という意味である。一方、ＬＡＮ３（３）とＬＡＮ４（４）はそれぞれＲＦＣ２６１５で規定されているＰＯＳ（PPP Over SONET）を用い、回線（１３）、（１４）を介してエッジルータ（１０）に接続されている。回線（１３）、（１４）とエッジルータの物理インターフェースをそれぞれ（１５）、（１６）とする。

【００１９】本実施例では、ＬＡＮ１とＬＡＮ２が属しているＶＰＮを識別する識別子としてＶＰＩ、ＶＣＩが用いられる。エッジルータ（９）内に設けられたＶＰＮ識別子設定テーブルにおいて、物理インターフェース（１２）に対応するエントリには、ＶＰＩ、ＶＣＩと設定される。エッジルータ（１０）は、ＬＡＮ３とＬＡＮ４が属しているＶＰＮを識別する識別子として物理インターフェースに与えられている番号を用いる。エッジルータ（１０）内に設けられたＶＰＮ識別子設定テーブルにおいて、物理インターフェース（１５）、（１６）に対応するエントリには、物理インターフェースと設定される。ＶＰＮ識別子設定テーブルは後述される。

【００２０】また、エッジルータ（９）内には、ＶＰＮ識別子と、当該ＶＰＮ識別子を有するパケットが何れのＶＰＮに属するかを示す情報（以下、ＶＰＮ番号という。）との対応関係を示すＶＰＮ識別テーブルが設けられている。上記ＶＰＮＡ、ＶＰＮＢがＶＰＮ番号に該当する。さらに、エッジルータ（９）内には、宛先ＩＰアドレスと、出力方路及び出力パケットのカプセルヘッダ情報との関係を示すルーティングテーブルが設けられている。このルーティングテーブルはＶＰＮＡ用のものと、ＶＰＮＢ用のものとが用意される。ＶＰＮ識別テーブル及びルーティングテーブルについても後述される。

【００２１】エッジルータ（９）は、ＬＡＮ１から送信されたＬＡＮ３宛のＩＰパケットを受信すると、ＶＰＮ識別子設定テーブルの設定に従い、ＶＰＮ識別子としてＶＰＩ、ＶＣＩを用いることを決定する。ＶＰＮ識別子を決定した後、エッジルータ（９）は、ＶＰＩ、ＶＣＩとＶＰＮとの対応が示されているＶＰＮ識別テーブルを検索し、当該パケットがＶＰＮＡに属するパケットであると判定する。次に、エッジルータ（９）は、宛先ＩＰアドレスを検索キーとしてＶＰＮＡ用のルーティングテーブルを検索し、次転送先のコアルータ（１７）を決定し、そして、コアルータ行きのＶＰＮＡに属するパケットのカプセルヘッダを決定する。このカプセルヘッダが付与されたパケットは、コアルータ（１７）へ転送される。

【００２２】コアルータ（１７）は、カプセルヘッダ、すなわち、ＶＰＩ、ＶＣＩと、次転送先との対応関係を示すルーティングテーブルを有しており、受信パケットのカプセルヘッダを検索キーにして次転送先（エッジルータ（１０））、および次のカプセルヘッダを決定し、前記カプセルヘッダを付与してエッジルータ（１０）へ送信する。

【００２３】エッジルータ（１０）は、エッジルータ（９）と同様の構成であり、エッジルータ（９）と同様にして、受信パケットのカプセルヘッダを検索キーにしてＶＰＮ識別を行い、ＶＰＮＡに属するパケットであることを判定する。次に宛先ＩＰアドレスを検索キーとしてＶＰＮＡ用のルーティングテーブルを検索して転送先を決定し、カプセルヘッダをはずしてＬＡＮ３へパケットを転送する。

【００２４】エッジルータ（９）は、物理インターフェースに多重された論理的なチャネル番号によりＶＰＮを識別し、当該ＶＰＮのルーティングテーブルを検索するので、一つの回線に論理的に多重されたＶＰＮを識別することが可能となる。また、これにより、企業Ａが用いるＩＰアドレスとと企業Ｂが用いるＩＰアドレスとがバッティングする場合でも、正しいあて先への転送が可能となる。

【００２５】ＶＰＮＢ内のＬＡＮ４からＬＡＮ２へパケ

ットを送信する場合も上記の場合と同様の手続により送信が行われるが、ＬＡＮ４から送信されたＬＡＮ２宛のＩＰパケットを受信したエッジルータ（１０）は、ＶＰＮ識別子として物理インターフェースを用いる点が上記の場合と異なる。

【００２６】図２は、図１に示される実施例の変形例を説明するための図である。本実施例では、ＬＡＮ１とＬＡＮ２は、別回線（１８）、（１９）を介して、直接、ＩＳＰネットワーク（５）内の多重化装置（２０）に収容される。多重化装置（２０）において、ＶＰＮＡ、ＶＰＮＢごとに異なるＶＰＩ、ＶＣＩが割り当てられる。エッジルータ（９）は、図１の場合と同様に、ＶＰＩ、ＶＣＩを用いてＶＰＮ識別を行う。

【００２７】図３は、図１に示される実施例の他の変形例を説明するための図である。

【００２８】図３では、図１に示したネットワーク構成に、ＬＡＮ５（２１）が付け加えられており、ＬＡＮ２、ＬＡＮ４及びＬＡＮ５の間でＶＰＮＢが構成されている。ＬＡＮ５（２１）はＰＯＳを用い、回線（２２）でエッジルータ（９）に接続されている。回線（２２）とエッジルータの物理インターフェースを（２３）とする。

【００２９】エッジルータ（９）は、図１の説明と同様に、ＬＡＮ１とＬＡＮ２が属しているＶＰＮを識別する識別子としてＶＰＩ、ＶＣＩを用いる。一方、エッジルータ（９）は、ＬＡＮ５が属しているＶＰＮを識別する識別子として物理インターフェースを用いる。エッジルータ（９）内のＶＰＮ識別子設定テーブルには、物理インターフェース（２３）に対応するエントリに物理インターフェースと設定される。本実施例では、エッジルータ（９）内に、ＶＰＩ、ＶＣＩとＶＰＮとの対応が示されているＶＰＮ識別テーブルと、物理インターフェースとＶＰＮとの対応が示されているＶＰＮ識別テーブルとの２種類のＶＰＮ識別テーブルが設けられている。その詳細は後述される。

【００３０】例えば、ＬＡＮ５から送信されたＬＡＮ４宛のＩＰパケットを受信した場合、エッジルータ（９）は、ＶＰＮ識別子設定テーブルの設定に従い、ＶＰＮ識別子として物理インターフェースの番号を用いることを決定する。ＶＰＮ識別子を決定した後、エッジルータ（９）は、物理インターフェースの番号を検索キーとして、物理インターフェースとＶＰＮとの対応が示されているＶＰＮ識別テーブルを検索し、そのＩＰパケットがＶＰＮＢに属するパケットであることを判定する。次に、宛先ＩＰアドレスを検索キーとしてＶＰＮＢ用のルーティングテーブルを検索し、次転送先のコアルータ（１７）を決定し、その決定したコアルータに送信されるパケットのカプセルヘッダを決定する。このカプセルヘッダをパケットに付与し、コアルータ（１７）に転送する。

【００３１】本実施例では、異なる下位プロトコル毎にＶＰＮ識別子を定め、各ＶＰＮ識別子対応にＶＰＮ識別テーブルを設けている。このようにすることにより、一つのルータで異なる下位プロトコルに対応する際の自由度が増す。すなわち、本実施例によれば、エッジルータに収容しようとする下位プロトコルに応じて、ＶＰＮ識別子設定テーブル内のＶＰＮ識別子を設定し、そのＶＰＮ識別子に対応するＶＰＮ識別テーブルを設定しさえすれば、エッジルータにおいて様々な下位プロトコルを収容することが可能となる。

【００３２】次に、本発明のＶＰＮエッジルータの詳細を説明する。ＶＰＮを構成する上で、ネットワークの構成は図１～図３に示したもの以外にも、多様な構成が考えられる。そこで、図１～図３のネットワークを構成する場合のＶＰＮエッジルータの構成に限定して説明するのではなく、より一般的に、本発明ＶＰＮエッジルータの構成を説明する。

【００３３】図４から図８を用いて、ＶＰＮエッジルータ（９）の一構成例を説明する。ＶＰＮエッジルータ（１０）の構成もこれと同様である。

【００３４】図４は、本発明のＶＰＮエッジルータ（９）の一構成例を示す図である。制御部（５０）は、下位レイヤ処理部（５３、５４）、パケットレイヤ処理部（５２）及びスイッチ（５１）と接続されており、ＶＰＮエッジルータ全体の制御及びルーティング処理などを行う。下位レイヤ処理部（５３、５４）は、回線（５５、５６）を収容するとともに、ＩＰの下位レイヤの終端を行う。パケットレイヤ処理部（５２）は、下位レイヤ処理部（５３、５４）から下位レイヤの情報及びＩＰパケットを受け取り、その下位レイヤの情報とそのＩＰパケットのヘッダ情報とを用いてパケットの転送先を決定する。スイッチ（５１）は複数の入出力ポートを有しており、それらのポートは、パケットレイヤ処理部と接続されている。スイッチ（５１）は、例えば、クロスバスイッチで構成される。スイッチ（５１）は、パケットレイヤ処理部（５２）からパケットを受信すると、パケットレイヤ処理部（５２）において決定されたパケットの転送先に対応する出力ポートに、そのパケットを出力する。前記制御部（５０）には制御端末（５７）が接続される。前記制御端末により、ルータの管理者は、ルータ内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル及びルーティングテーブルの設定等を行うことが可能である。受信回線５５－１、５５－２、５５－３及び５５－４とルータ（９）との接続点には、それぞれ、物理インタフェース番号１、２、３及び４が割り当てられている。

【００３５】図５は、パケットレイヤ処理部（５２）の一構成例を示す図である。下位レイヤ処理部ＩＦ（１００、１０６）、スイッチＩＦ（１０３、１０４）及び制御部ＩＦ（１１０）は、それぞれ、下位レイヤ処理部

（５３、５４）とのインタフェース、スイッチ（５１）とのインタフェース及び制御部（５０）とのインタフェースである。本実施例の特徴の一つは、ＶＰＮ識別子設定テーブル（１５０）、ＶＰＮ識別テーブル（１５１）及びＶＰＮ用のルーティングテーブル（１５２）を設けた点にある。これらはメモリ上に構成される。これらは、それぞれ、物理的に異なるメモリ上に構成されてもよいし、同一のメモリ上の異なる領域に構成されてもよい。この構成の仕方の差異は本発明を実施する上で本質的なものではない。ＶＰＮ識別子設定テーブル（１５０）、ＶＰＮ識別テーブル（１５１）、ルーティングテーブル（１５２）及びここで説明しなかったその他のブロックの機能・構成は、以下で説明するルータ（９）のパケット処理動作と併せて説明する。

【００３６】下位レイヤ処理部（５３）が収容している回線（５５）からパケットを受信し、下位レイヤ処理部（５４）が収容している回線（５６）へパケットを転送する場合を例に引き、ルータ（９）のパケット処理を説明する。

【００３７】下位レイヤ処理部（５３）は、ＬＡＮからパケットを受信すると、ＩＰの下位レイヤのプロトコルを終端する。下位レイヤ処理部（５３）は、ＩＰパケットとともに、パケットを受信した物理インターフェース番号（以下、受信物理インターフェース番号と呼ぶ）、下位レイヤのプロトコル種別、ＶＰＮ識別子として用いる下位レイヤのカプセルヘッダ情報等をパケットレイヤ処理部（５２）へ転送する。

【００３８】パケットレイヤ処理部（５２）内の下位レイヤ処理部インターフェース（１００）は、下位レイヤ処理部（５３）から転送されたＩＰパケット、受信物理インターフェース番号、下位レイヤのプロトコル種別及びＶＰＮ識別子として用いる下位レイヤのカプセルヘッダ情報をパケット転送処理部（１０１）へ転送する。パケット転送処理部（１０１）は、受信したＩＰパケットからＩＰヘッダ情報を抽出し、このＩＰヘッダ情報、受信物理インターフェース番号、下位レイヤのプロトコル種別及びＶＰＮ識別子として用いる下位レイヤのカプセルヘッダ情報をＶＰＮ識別・ルーティングテーブル検索処理部（１０２）へ転送する。ＩＰパケット本体はパケット転送処理部（１０１）内に一時的に蓄積される。

【００３９】ＶＰＮ識別・ルーティングテーブル検索処理部（１０２）は、まず受信物理インターフェース番号、下位レイヤのプロトコル種別等を検索キーとしてＶＰＮ識別子設定テーブル（１５０）を検索し、ＶＰＮ識別子を決定する。

【００４０】図６は、ＶＰＮ識別子設定テーブル（１５０）の一構成例を示す。各エントリは、物理インターフェース番号（２００）、下位レイヤプロトコル（２０３）及びＶＰＮ識別子（２０１）とを有する。下位レイヤプロトコルがＡＴＭのエントリには、パケットの転送優先度を示すＣＬＰのフィールドを設けてあるが、このフィールドはなくてもよい。上述の通り、エッジルータ（９）の管理者は、制御端末（５７）から、ＶＰＮ識別子を設定することができる。ＶＰＮ識別・ルーティングテーブル検索処理部（１０２）は、検索キーとして受信物理インターフェース番号を用いて検索を行い、ＶＰＮ識別子（２０１）を決定する。例えば、受信物理インタフェース番号が１の場合、ＶＰＮ識別子はＶＰＩ、ＶＣＩとなり、受信物理インタフェース番号が３の場合、ＶＰＮ識別子は物理インタフェース番号となる。本実施例のように、ＣＬＰフィールドを設ける場合には、ＶＰＮ識別子として、ＶＰＩ、ＶＣＩとＣＬＰとの組み合わせ、物理インタフェース番号とＣＬＰとの組み合わせを用いてもよい。ＶＰＮ識別子にＣＬＰ（２０４）を含めた場合のメリットについては後述する。一つの物理インタフェースに対して、複数のＶＰＮに属するパケットが論理的に多重されて送信される場合、受信物理インタフェース番号からは、そのパケットがどのＶＰＮに属するのか判別することができない。しかし、その下位レイヤがＡＴＭの場合、ＶＰＩ、ＶＣＩをＶＰＮ識別子に用いれば、そのパケットがどのＶＰＮに属するのかを識別することが可能となる。一つの物理インタフェースに対して、一つのＶＰＮに属するパケットしか送信されない場合には、物理インタフェース番号でＶＰＮを識別することが可能である。検索キーとして、下位レイヤのプロトコル（２０３）と物理インターフェース番号（２０１）との組み合わせを用いてもよい。例えば、物理インターフェース番号４に接続される回線が時分割多重回線であり、前記回線に、下位レイヤのプロトコルとしてフレームリレーを用いたパケットと、ＰＰＰ(Point to Point Protocol)プロトコルを用いたパケットが多重されているとする。また、下位レイヤプロトコルがフレームリレーのエントリに対しては、ＶＰＮ識別キーとしてＤＬＣＩが設定されており、下位レイヤプロトコルがＰＰＰのエントリに対しては、ＶＰＮ識別キーとしてタイムスロット番号が設定されているとする。この場合、受信物理インタフェース番号４のみを検索キーとして検索しても、ＶＰＮ識別子がＤＬＣＩであるかタイムスロット番号であるかが一意に定まらない。そこで、この場合には、受信物理インタフェース番号と下位レイヤプロトコルとの組み合わせにより、ＶＰＮ識別子を検索する。

【００４１】ＶＰＮ識別子が決定されると、ＶＰＮ識別・ルーティングテーブル検索処理部は、そのＶＰＮ識別子を検索キーとしてＶＰＮ識別テーブル（１５１）を検索し、受信パケットが属しているＶＰＮを決定する。

【００４２】図７（ａ）、（ｂ）は、ＶＰＮ識別テーブル（１５１）の一構成例を示す。どちらのＶＰＮ識別テーブルにおいても、各エントリは、ＶＰＮ識別子（２０１）とＶＰＮ番号（２５０）とを有する。

【００４３】図７（ａ）は、ＶＰＮ識別子（２０１）と

してＶＰＩ、ＶＣＩを用いるテーブルの例を示している。図７（ａ）のＣＬＰフィールド（２０４）及び装置内優先度情報フィールド（２５１）は設けなくても良い。装置内優先度情報フィールド（２５１）とは、装置内におけるパケット処理の優先度情報を示すフィールドである。ＶＰＮ識別・ルーティングテーブル検索処理部（１０２）は、検索キーとして前記のＶＰＮ識別子設定テーブルの検索により決定したＶＰＮ識別子に従い、検索キーとしてパケットヘッダ内のＶＰＮ識別情報を用いて検索を行い、ＶＰＮ番号（２５０）を決定する。本実施例のように、ＶＰＮ識別テーブル（１５１）にＣＬＰフィールド（２０４）及び装置内優先度情報フィールド（２５１）を設ける場合には、検索キーとしては、パケットの転送優先度を示すＣＬＰ（２０４）とＶＰＩ、ＶＣＩの組み合わせを用いてもよい。ＣＬＰを検索キーに含めることにより、同一のＶＰＮ番号に属するパケットに対して、異なる装置内優先度情報を定めることができる。例えば、”ＶＰＩ、ＶＣＩ＝ａ”かつ”ＣＬＰ＝０”の場合は、”装置内優先度＝ａ”、”ＶＰＩ、ＶＣＩ＝ａ”かつ”ＣＬＰ＝１”の場合は、”装置内優先度＝ｂ”のように、同一のＶＰＮ番号に属するパケットに対して異なる装置内優先度情報を定めることができる。

【００４４】図７（ｂ）は、ＶＰＮ識別子（２０１）として物理インターフェース番号（２５２）を用いるテーブルの例を示している。パケット処理の優先制御を行わないのであれば、図７（ｂ）の装置内優先度情報フィールド（２５１）は設けなくても良い。

【００４５】上記以外のＶＰＮ識別子、例えば、ＤＬＣＩ、タイムスロット番号等が使用される場合には、図７（ａ）、（ｂ）と同様のテーブルを構成すればよい。すなわち、ＶＰＮ識別テーブル（１５１）は、ＶＰＮ識別子毎に設けられ、これらの設定は、制御端末（５４）から設定される。ＶＰＮ識別子毎に設けられたＶＰＮ識別テーブル（１５１）は、同一のメモリ上に構成されても良いし、それぞれ、異なるメモリ上に構成されてもよい。

【００４６】ＶＰＮ番号が決定されると、ＶＰＮ識別・ルーティングテーブル検索処理部は、そのＶＰＮ番号に対応するＶＰＮ用のルーティングテーブル（１５２）を検索し、出力方路及びそのＶＰＮ番号に属するパケットに付加されるＶＰＮ用の出力カプセルヘッダ情報を決定する。

【００４７】図８は、ＶＰＮ用ルーティングテーブル（１５２）の一構成例を示す。ＶＰＮ識別・ルーティングテーブル検索処理部（１０２）は、収容するＶＰＮ毎にこのＶＰＮ用ルーティングテーブル（１５２）を保持する。このＶＰＮ毎に設けられたＶＰＮ用ルーティングテーブル（１５２）は、同一のメモリ上に構成されても良いし、それぞれ異なるメモリ上に構成されてもよい。ＶＰＮ用ルーティングテーブル（１５２）は宛先ＩＰアドレス（３００）と出力方路番号（３０１）と出力カプセルヘッダ情報（３０２）とを有する。出力方路番号（３０１）は、スイッチ等でパケットを所望のインターフェースに転送するための装置内識別子である。出力カプセルヘッダ情報（３０２）は、ＩＳＰネットワーク（５）内で用いるカプセルヘッダ情報である。ＶＰＮ識別・ルーティングテーブル検索処理部（１０２）は、検索キーとしてＩＰヘッダ内の宛先ＩＰアドレスを用いて、前記のＶＰＮ識別テーブルの検索により決定したＶＰＮ番号（２５０）に対応するＶＰＮ用のルーティングテーブルの検索を行い、出力方路番号（３０１）及び出力カプセルヘッダ情報（３０２）を決定する。本実施例では、ＶＰＮ毎にＶＰＮ用ルーティングテーブル（１５２）を設けているので、複数のＶＰＮにおいて同一のＩＰアドレスが使用されていても、正しい出力方路を決定することができる。

【００４８】出力方路番号（３０１）と出力カプセルヘッダ情報（３０２）とが決定されると、ＶＰＮ識別・ルーティングテーブル検索処理部（１０２）は、その決定した出力方路（３０１）と出力カプセルヘッダ情報（３０２）とをパケット転送処理部（１０１）に転送する。

【００４９】パケット転送処理部（１０１）は、スイッチＩＦ（１０３）を介して、蓄積していたＩＰパケット本体、出力方路番号（３０１）及び出力カプセルヘッダ情報（３０２）とをスイッチ（５１）に転送する。スイッチ（５１）は、パケット転送処理部（１０１）から受信したＩＰパケット本体と、その出力カプセルヘッダ情報（３０２）とを、その出力方路番号に対応する出力ポートに出力する。

【００５０】上記出力ポートに接続されているパケットレイヤ処理部（５２）、すなわち、パケットレイヤ処理部（５２）から送信されたＩＰパケット本体及びその出力カプセルヘッダ情報（３０２）を受信する側のパケットレイヤ処理部（５２）は、スイッチＩＦ（１０４）を介して、それらを受信する。ＩＰパケット本体及びその出力カプセルヘッダ情報（３０２）とを受信すると、パケット転送処理部（１０５）はこれらを下位レイヤ処理部ＩＦ（１０６）を介して下位レイヤ処理部（５４）に転送する。ＩＰパケット本体及びその出力カプセルヘッダ情報（３０２）とを受信すると、下位レイヤ処理部（５４）は、その出力カプセルヘッダ情報に基づきカプセルヘッダを生成し、そのカプセルヘッダによりＩＰパケット本体をカプセル化し、そして、そのカプセル化したパケットをコアルータ（１７）に送信する。

【００５１】以上、図４から図８を用いてＶＰＮエッジルータ装置の一構成例を説明した。本実施例のルータ装置を用いることにより、同一の物理インタフェースに、異なるＶＰＮに属するパケットが送信される場合であっても、それらが属するＶＰＮを識別することが可能となる。また、同一のエッジルータが、異なるＩＰの下位プ

ロトコルを用いる複数のＬＡＮを収容する場合でも、それぞれの下位プロトコルに対応した適切なＶＰＮ識別子をＶＰＮ識別子設定テーブルに設定することができるので、ＶＰＮ構築の自由度が増す。

【００５２】本実施例では、ＶＰＮ用ルーティングテーブルの検索結果として出力カプセルヘッダ情報を直接出力しているが、出力カプセル番号を出力するようにしてもよい。この出力カプセル番号は、出力側の下位レイヤ処理部においてカプセルヘッダを付与するための装置内識別子である。この場合、出力側の下位レイヤ処理部にカプセル番号とカプセルヘッダとをペアにしたヘッダ生成テーブルを設ける。出力側の下位レイヤ処理部は、検索キーとそてカプセル番号を用いてヘッダ生成テーブルを検索し、カプセルヘッダを決定する。

【００５３】本実施例で示したテーブルは論理的なテーブルであり、テーブル検索方法として、ツリー構造に代表される検索アルゴリズムを用いてもよいし、ＣＡＭ（Content Addressable Memory）を使った構成や、テーブルを逐次検索していく方式を採用してもよい。

【００５４】ＶＰＮエッジルータ装置が時分割多重回線を収容する場合、下位レイヤ処理部がパケットレイヤ処理部に転送する情報として、本実施例で説明した各情報の他、タイムスロット番号を加えてもよい。この場合、ＶＰＮ識別子として、ＶＰＮ識別子設定テーブルにタイムスロット番号を設定してもよい。また、ＶＰＮ識別テーブルの検索キーとして、タイムスロット番号を用いてもよい。

【００５５】ＶＰＮエッジルータ装置がイーサネットを収容し、イーサネット上のパケットがIEEE802.1Qに従ってＶＬＡＮカプセル化されている場合、下位レイヤ処理部がパケットレイヤ処理部に転送する情報として、本実施例で説明した各情報の他、ＶＬＡＮ　Ｔａｇ情報を加えてもよい。この場合、ＶＰＮ識別子として、ＶＰＮ識別子設定テーブルにＶＬＡＮ　Ｔａｇ情報を設定してもよい。また、ＶＰＮ識別テーブルの検索キーとして、ＶＬＡＮ　Ｔａｇ情報を用いてもよい。

【００５６】ＩＰパケットがＬ２ＴＰ（Layer2 Tunneling Protocol）で規定されているＬ２ＴＰヘッダでカプセル化されている場合、ＶＰＮ識別子として、ＶＰＮ識別子設定テーブルにL2TPカプセルヘッダ内の各情報（トンネルID、セッションID等）を設定してもよい。

【００５７】また、IPパケットがPPP Over Ethernetカプセル化方式で規定されているカプセル情報でカプセル化されている場合、下位レイヤ処理部がパケットレイヤ処理部に転送する情報として、本実施例で説明した各情報の他、PPP Over Ethernetカプセル化方式で規定されているカプセル情報を加えてもよい。この場合、ＶＰＮ識別子として、ＶＰＮ識別子設定テーブルにPPP Over Ethernetカプセル化方式で規定されているカプセル情報（セッションID等）を設定してもよい。

【００５８】図９は、本発明のＶＰＮエッジルータ装置（９）の他の構成例を示す。インターフェースカード（４００、４０１）は、それぞれ、同一の下位レイヤのプロトコルを用いる回線を収容するカードである。例えばインターフェースカード（４００）はＡＴＭ用のインターフェースカードであり、ＡＴＭ回線（４０２）を収容する。また、インターフェースカード（４０１）はＰＯＳ用のインターフェースカードであり、ＰＯＳ回線（４０３）を収容する。インターフェースカード（４００、４０１）は着脱可能であり、ルータの管理者は、必要な下位レイヤプロトコル用のインターフェースカードを必要な数量だけ搭載することができる。各インターフェースカードには、各下位レイヤプロトコルに特有の処理を行う下位レイヤ処理部（４０５、４０６）が搭載されている。下位レイヤ処理部（４０５、４０６）の動作は、図４の下位レイヤ処理部（５３、５４）と同様である。パケット処理カード（４０７）は前記インターフェースカードからＩＰパケット等の情報を受け取り、パケットレイヤ処理を行うカードである。各パケット処理カード（４０７）は着脱可能であり、ルータの管理者は、必要な数量だけ搭載することができる。各パケット処理カード（４０７）には、図４、図５を用いて説明したパケットレイヤ処理部（５２）が搭載されている。管理者は、収容するインタフェースカードの種別、ＬＡＮとインタフェースカードとの間のアクセス網の構成に応じて、制御端末（５７）から、パケット処理カード（４０７）内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの構成をフレキシブルに設定することができる。本実施例のＶＰＮエッジルータ装置のパケット処理動作は、図４から図８を用いて説明した動作と同様である。

【００５９】図１０から図１２は、図９のパケット処理カード（４０７）に収容されるインタフェースカードと、パケット処理カードに保持されるＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルとの関係を示す図である。図１０から図１２は、エッジルータに収容されるＬＡＮと、エッジルータ（９）の構成要素のうちインターフェースカードとパケット処理カードのみを示す。また、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルは論理的なものである。図１０から図１２では、同一インターフェースカード内の全物理インターフェースに対し、同じＶＰＮ識別子が使用される場合を示している。このため、ＶＰＮ識別子設定テーブルの検索キーとして物理インターフェース番号を設定する必要がないので、図１０から図１２では、その検索キーとしての物理インターフェース番号は省略されている。同一インターフェースカード内で、異なるＶＰＮ識別子が使用される場合は、上述のようにＶＰＮ識別子設定テーブルの検索キーとして物理インターフェ

ースを用いればよい。

【００６０】図１０は、パケット処理カード（４０７）にＡＴＭ用インターフェースカード（４００）が収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す。ＬＡＮ１（４５０）はＶＰＮＡに属し、ＬＡＮ２（４５１）はＶＰＮＢに属しているとする。ＬＡＮ１、ＬＡＮ２からのパケットは多重化装置（４５２）で多重され、回線（４５３）を介してＡＴＭ用インターフェースカード（４００）に収容される。多重される際、ＬＡＮ１、ＬＡＮ２からのパケットにはＶＰＩ、ＶＣＩとしてそれぞれａ、ｂという値が割り当てられているとする。本実施例では、ＶＰＮ識別にはＶＰＩ、ＶＣＩを用いる。パケット処理カード（４０７）内のＶＰＮ識別子設定テーブル（４５５）にはＶＰＮ識別子としてＶＰＩ、ＶＣＩが設定される。ＶＰＮ識別テーブル（４５６）には検索キーとしてＶＰＩ、ＶＣＩが設定される。ＶＰＮ用ルーティングテーブルとしてはＶＰＮＡ用ルーティングテーブル（４５７）、ＶＰＮＢ用ルーティングテーブル（４５８）が設けられる。例えば、ＬＡＮ１からパケットを受信すると、ＡＴＭ用インターフェースカード（４００）内の下位レイヤ処理部（４０５）は、ＡＴＭプロトコルを終端し、ＩＰパケット本体及びＶＰＩ、ＶＣＩ、物理インターフェース番号等をパケット処理カード（４０７）に転送する。パケット処理カード（４０７）内のＶＰＮ識別・ルーティングテーブル検索処理部は、ＶＰＮ識別子設定テーブル（４５５）を検索し、ＶＰＮ識別子としてＶＰＩ、ＶＣＩを用いることを決定する。次に、受信パケットのＶＰＩ、ＶＣＩの値、”ａ”、を用いてＶＰＮ識別テーブル（４５６）を検索し、受信パケットがＶＰＮＡに属することを判定する。次にＶＰＮＡ用のルーティングテーブル（４５７）を検索し、出力方路、および出力カプセルヘッダ情報を決定する。

【００６１】図１１は、パケット処理カード（４０７）にＰＯＳ用インターフェースカード（４０１）が収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す。

【００６２】ＬＡＮ１（４５０）はＶＰＮＡに属し、ＬＡＮ２（４５１）はＶＰＮＢに属しているとする。ＬＡＮ１、ＬＡＮ２はそれぞれ回線（５００）、（５０１）を介してＰＯＳ用インターフェースカード（４０１）に収容される。回線（５００）及び回線（５０１）とＰＯＳ用インターフェースカード（４０１）との物理インターフェース番号をそれぞれ１、２とする。この場合、ＶＰＮ識別には物理インターフェースを用いるため、パケット処理カード（４０７）内のＶＰＮ識別子設定テーブル（４５５）にはＶＰＮ識別子として物理インターフェース番号が設定される。ＶＰＮ識別テーブル（４５６）には検索キーとして物理インターフェース番号を設定する。ＶＰＮ用ルーティングテーブルとして、ＶＰＮＡ用ルーティングテーブル（４５７）、ＶＰＮＢ用ルーティングテーブル（４５８）が設けられる。パケット処理カード（４０７）内の処理は、図１０を用いて説明した処理と同様である。ただし、ＶＰＮ識別子としてＶＰＩ、ＶＣＩではなく、物理インターフェースを用いる点が異なる。

【００６３】図１２は、図９に図示していないが、パケット処理カード（４０７）に時分割多重回線用のインターフェースカード（５５０）が収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す。ＬＡＮ１（４５０）、ＬＡＮ２（４５１）、ＬＡＮ３（５５１）ＬＡＮ４（５５２）はそれぞれＶＰＮＡ、ＶＰＮＢ、ＶＰＮＣ、ＶＰＮＤに属しているとする。ＬＡＮ１、ＬＡＮ２の下位プロトコルはフレームリレーとし、ＬＡＮ３、ＬＡＮ４の下位プロトコルはＰＰＰ（Point to Point Protocol）とする。ＬＡＮ１とＬＡＮ２からのパケットにはＤＬＣＩとしてそれぞれ１０、２０が割り当てられ、それらのパケットは、フレームリレー多重化装置（５５３）において、回線（５５４）に多重化される。さらに、時分割多重化装置（５５５）において、回線（５５４）、（５５６）、（５５７）が回線（５５８）に多重される。この際、回線（５５４）、（５５６）、（５５７）のデータにはそれぞれ、タイムスロット番号１、２、３が割り当てられるとする。ＬＡＮ１、ＬＡＮ２に対するＶＰＮ識別子としてはＤＬＣＩが用いられ、ＬＡＮ３、ＬＡＮ４に対するＶＰＮ識別子としてはタイムスロット番号が用いられるとする。この場合、ＶＰＮ識別子設定テーブル（４５５）における、下位レイヤプロトコル（５５９）がフレームリレーであるエントリに対しては、ＶＰＮ識別子としてＤＬＣＩ（５６０）が設定される。また、下位レイヤがＰＰＰであるエントリに対してはＶＰＮ識別子としてタイムスロット番号（５６１）が設定される。ＶＰＮ識別テーブルとして、２つのテーブル、すなわち、ＤＬＣＩとＶＰＮ番号の対応を示すＶＰＮ識別テーブル（５６２）と、タイムスロット番号とＶＰＮ番号の対応を示すＶＰＮ識別テーブル（５６３）とが設けられる。また、ＶＰＮ用ルーティングテーブルとして、ＶＰＮＡ用ルーティングテーブル（４５７）、ＶＰＮＢ用ルーティングテーブル（４５８）、ＶＰＮＣ用ルーティングテーブル（５６４）及びＶＰＮＤ用ルーティングテーブル（５６５）が設けられる。パケット処理カード（４０７）内の処理は、図１０を用いて説明した処理と同様である。ただし、ＶＰＮ識別子設定テーブル検索時に、検索キーとして下位レイヤプロトコル（５５９）を用いる点が異なる。またＶＰＮ識別子設定テーブル検索の結果、ＶＰＮ識別子として、ＬＡＮ１、ＬＡＮ２から受信

したパケットに関してはＤＬＣＩが使用され、ＬＡＮ３、ＬＡＮ４から受信したパケットに関してはタイムスロット番号が使用される点が異なる。

【００６４】図９から図１２では、１つのパケット処理カードが１つのインターフェースカードを収容する例について説明したが、パケット処理カードが複数のインターフェースカードを収容する構成をとってもよい。その際、収容する複数のインターフェースカードが異なる下位プロトコル用のものであってもよい。

【００６５】図１３は、パケット処理カード（４０７）に異なる下位プロトコル用のインターフェースカードが収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す。インターフェースカード（４００）、（４０１）はそれぞれＡＴＭ用、ＰＯＳ用とする。図１３は、同一インターフェースカード内の全物理インターフェースに対し、ＶＰＮ識別子が同じ場合を示している。本実施例で、パケット転送カードは複数のインターフェースカードを収容するため、各インターフェースカード（４００）、（４０１）にはそれぞれカード番号１、２が割り当てられている。また、ＶＰＮ識別子設定テーブル（４５５）の検索キーとして、カード番号（６０２）が設定される。ＬＡＮ１（４５０）、ＬＡＮ２（４５１）、ＬＡＮ３（５５１）ＬＡＮ４（５５２）はそれぞれＶＰＮＡ、ＶＰＮＢ、ＶＰＮＣ、ＶＰＮＤに属しているとする。ＬＡＮ１、ＬＡＮ２からのパケットは多重化装置（４５２）で多重され、回線（４５３）を介してＡＴＭ用インターフェースカード（４００）に収容される。多重される際、ＬＡＮ１、ＬＡＮ２からのパケットにはＶＰＩ、ＶＣＩとしてそれぞれａ、ｂという値が割り当てられるものとする。この場合、ＶＰＮ識別にはＶＰＩ、ＶＣＩを用いればよい。ＶＰＮ識別子設定テーブル（４５５）における、カード番号１のエントリ（６０３）に対しては、ＶＰＮ識別子としてＶＰＩ、ＶＣＩが設定される。ＬＡＮ３、ＬＡＮ４はそれぞれ回線（５００）、（５０１）を介してＰＯＳ用インターフェースカード（４０１）に収容される。回線（５００）、（５０１）とＰＯＳ用インターフェースカード（４０１）との物理インターフェース番号をそれぞれ１、２とする。この場合、ＶＰＮ識別には物理インターフェースを用いればよい。ＶＰＮ識別子設定テーブル（４５５）における、カード番号２のエントリ（６０４）に対しては、ＶＰＮ識別子として物理インターフェースが設定される。ＶＰＮ識別テーブルとしては、ＶＰＩ、ＶＣＩとＶＰＮ番号の対応を示すテーブル（６００）と、物理インターフェース番号とＶＰＮ番号の対応を示すテーブル（６０１）とが設けられる。ＶＰＮ用ルーティングテーブルとしてはＶＰＮＡ用ルーティングテーブル（４５７）、ＶＰＮＢ用ルーティングテーブル（４５８）、ＶＰＮＣ用ルーティングテーブル（５６４）、ＶＰＮＤ用ルーティングテーブル（５６５）とが設けられる。パケット処理カード（４０７）内の処理は、図１０を用いて説明した処理と同様である。ただし、ＶＰＮ識別子設定テーブル検索時に、検索キーとしてカード番号（６０２）を用いる点が異なる。ここでは、ＡＴＭとＰＯＳとを収容する場合を示したが、この組み合わせに限られるものではない。例えば、ＰＯＳ用インタフェースカードをＦＲ用インタフェースカードに換えることも可能である。この場合、ＬＡＮ３及びＬＡＮ４からのパケットは、ＬＡＮ１及びＬＡＮ２と同様に、一本の回線に多重してＦＲ用インタフェースカードに入力されるように、ＤＬＣＩでＶＰＮを識別するようにしてもよい。

【００６６】以上、図９から図１３を用いて説明したように、本実施例のルータ装置によれば、管理者は、収容するインタフェースカードの種別に応じて、制御端末（５７）から、パケット処理カード（４０７）内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの構成をフレキシブルに設定することができる。また、物理インターフェースに多重された論理的なチャネル番号によりＶＰＮを識別するので、一つの回線に論理的に多重されたＶＰＮを識別することが可能となる。

【００６７】図１４に、インタフェースカードを装着する際の、パケット処理カード（４０７）の設定手順の一例を示す。ＶＰＮエッジルータ（９）にインタフェースカードが装着された後、パケット処理カード（４０７）内のＶＰＮ識別子設定テーブル（４５５）が設定される（７０１、７０２）。ＶＰＮ識別子設定テーブルの設定は、装着するインタフェースカードの種別により、管理者が自由に設定することができる。次に、設定されたＶＰＮ識別子毎に、ＶＰＮ識別テーブルが設定される（７０３）。ＶＰＮ毎にルーティングテーブルが設定される（７０４）。

【００６８】ＶＰＮ識別子の設定は、インターフェースカードをパケット処理カードに装着する際に、インターフェースカードとパケット処理カード間で通信を行い、インターフェースカードが終端するＩＰパケットの下位レイヤのプロトコルを自動的に判定してパケット処理カードに通知するようにしてもよい。その通知された下位レイヤのプロトコルに対応して規定された識別情報を、ＶＰＮ識別子設定テーブルに自動設定することができる。

【００６９】以上、図１～図１４を用いて本発明のＶＰＮエッジルータの動作を説明した。これらに共通する動作フローを図１５に示す。

【００７０】ＶＰＮエッジルータは、ＬＡＮからＩＰパケットをカプセル化したパケットを受信すると（８０１）、ＶＰＮ識別子設定テーブルを検索し（８０２）、受信パケットのＶＰＮ識別子を決定する（８０３）。Ｖ

ＰＮ識別子としては、ＶＰＩ、ＶＣＩ等、論理的なチャネル識別子を用いるが、収容する下位プロトコルに応じて、これと物理インタフェース番号等とを組み合わせて使用してもよい。次に、決定したＶＰＮ識別子を検索キーとして、ＶＰＮ識別テーブルを検索し（８０４）、受信パケットが属するＶＰＮを決定する（８０５）。例えば、ＶＰＮ識別子がＶＰＩ、ＶＣＩである場合には、受信パケットに割り当てられたＶＰＩ、ＶＣＩを検索キーとして、ＶＰＮ識別テーブルを検索し、受信パケットが属するＶＰＮを決定する。決定されたＶＰＮ用のルーティングテーブルを検索し（８０６）、出力方路および出力用カプセルヘッダを決定する（８０７）。

【００７１】

【発明の効果】本発明のルータを用いることにより、物理インターフェースに多重化されている論理的なチャネル番号を用いてＶＰＮを識別することができる。従って、物理回線を増やすことなく、収容するＶＰＮの数を増やすことができる。

【００７２】また、ルータが収容する複数のＬＡＮがそれぞれ異なるＩＰの下位プロトコルを用いる場合でも、それぞれのプロトコルに対応した適切なＶＰＮ識別子を設定することができるので、ＶＰＮ識別を行うことができる。

【図面の簡単な説明】

【図１】本発明のＶＰＮエッジルータを用いて構成したＶＰＮの一実施例を説明するための図である。

【図２】図１に示される実施例の変形例を説明するための図である。

【図３】図１に示される実施例の他の変形例を説明するための図である。

【図４】本発明のＶＰＮエッジルータの一構成例を示す図である。

【図５】パケットレイヤ処理部の一構成例を示す図である。

【図６】ＶＰＮ識別子設定テーブル（１５０）の一構成例を示す図である。

【図７】ＶＰＮ識別テーブルの一構成例を示す図である。

【図８】ＶＰＮ用ルーティングテーブルの一構成例を示す図である。

【図９】本発明のＶＰＮエッジルータ装置の他の構成例を示す図である。

【図１０】パケット処理カードにＡＴＭ用インターフェースカードが収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す図である。

【図１１】パケット処理カードにＰＯＳ用インターフェースカードが収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す図である。

【図１２】パケット処理カードに時分割多重回線用のインターフェースカードが収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す図である。

【図１３】パケット処理カードに異なる下位プロトコル用のインターフェースカードが収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す図である。

【図１４】パケット処理カードの設定手順の一例を示す図である。

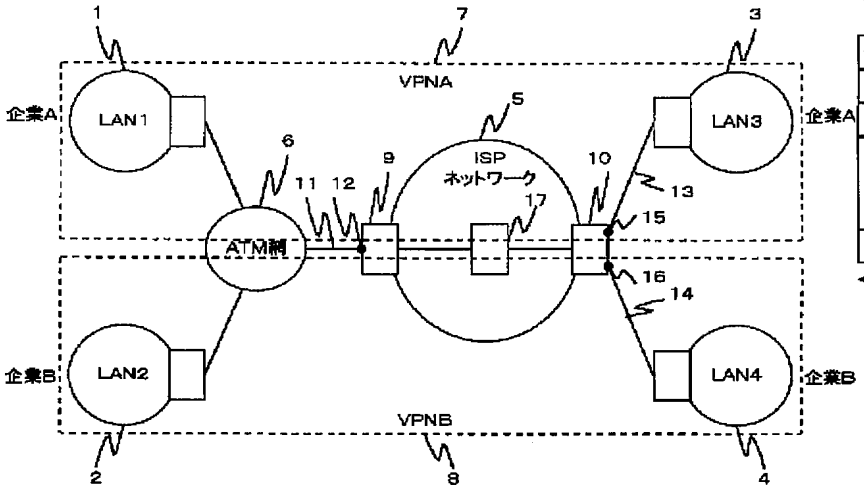
【図１５】本発明のＶＰＮエッジルータの動作フローを示すフローチャートである。

【符号の説明】

５…ＩＳＰネットワーク、９…ＶＰＮエッジルータ、５０…制御部、５１…スイッチ、５２…パケットレイヤ処理部、５３、５４…下位レイヤ処理部、１０１、１０５…パケット転送処理部、１０２…ＶＰＮ識別・ルーティングテーブル検索処理部、１５０…ＶＰＮ識別子設定テーブル、１５１…ＶＰＮ識別テーブル、１５２…ルーティングテーブル、４００…ＡＴＭ用インターフェースカード、４０１…ＰＯＳ用インターフェースカード、４０７…パケット処理カード。

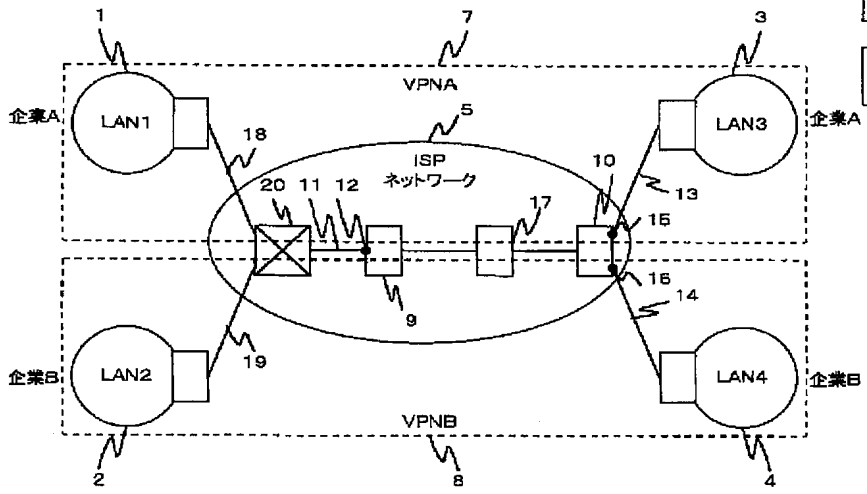
【図１】

図1



【図２】

図2



【図８】

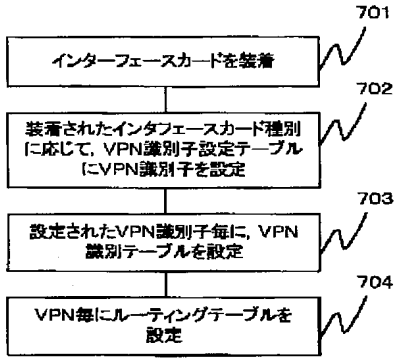
図8

300 宛先IPアドレス	301 出力方路番号	302 出力カプセルヘッダ情報
a. a. a. a	10	a
b. b. b. b	11	b
⋮	⋮	⋮
n. n. n. n	15	n

検索キー　　検索結果

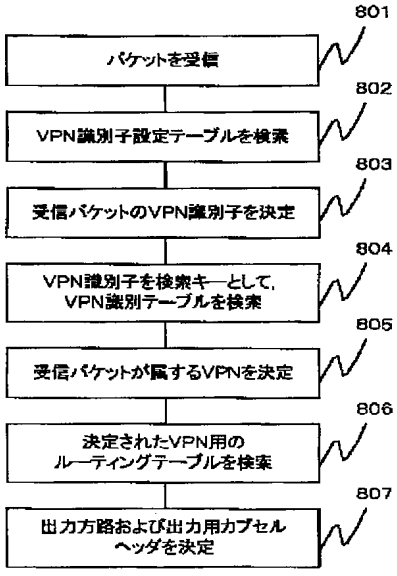
【図１４】

図14



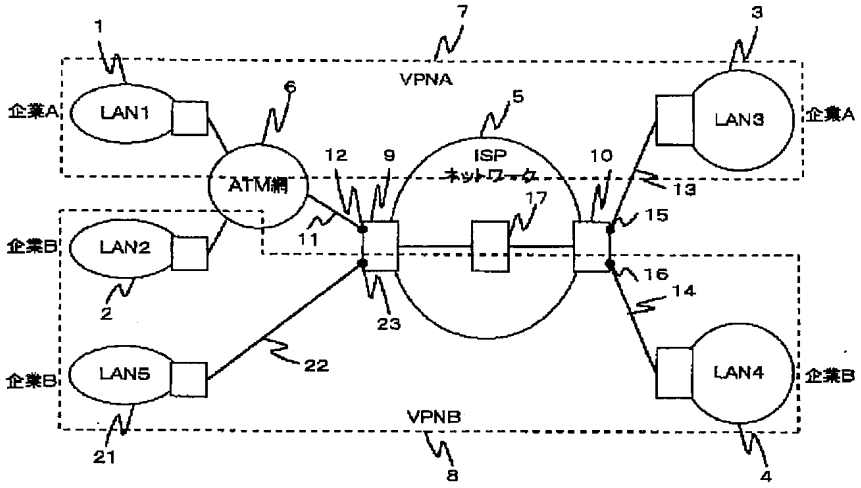
【図１５】

図15



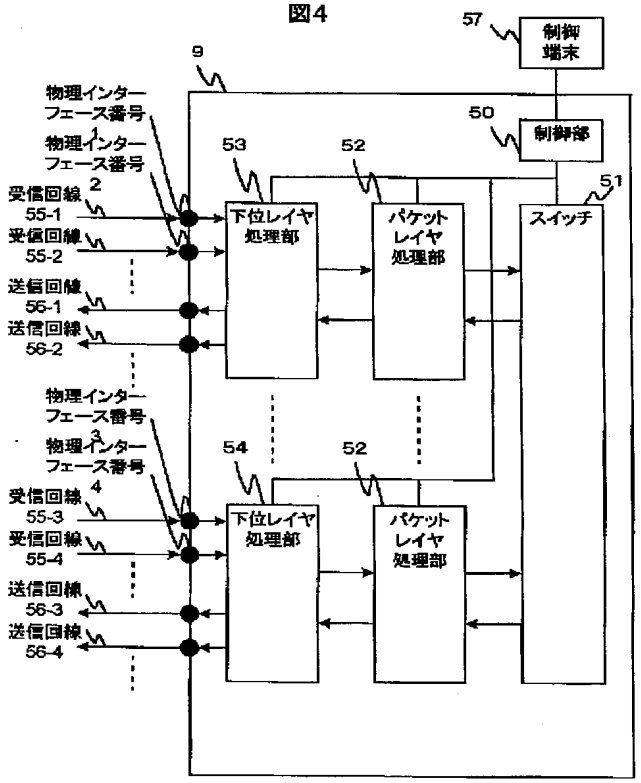
【図３】

図3



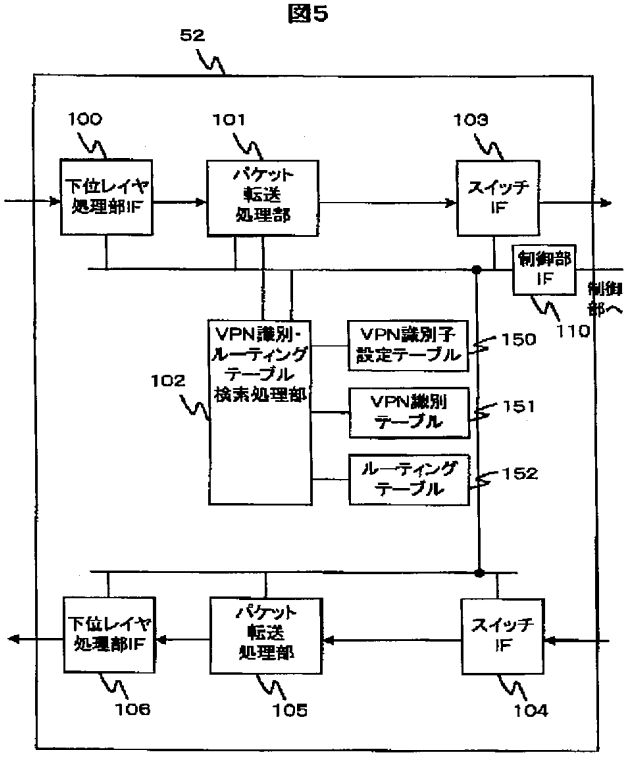
【図４】

図4



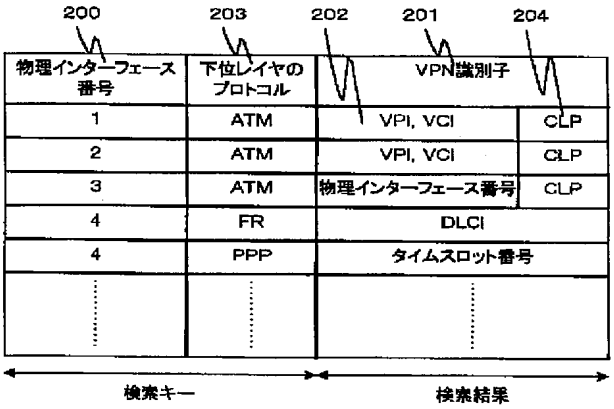
【図５】

図5



【図６】

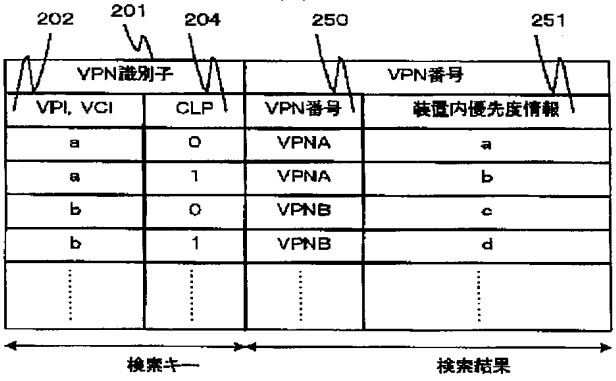
図6



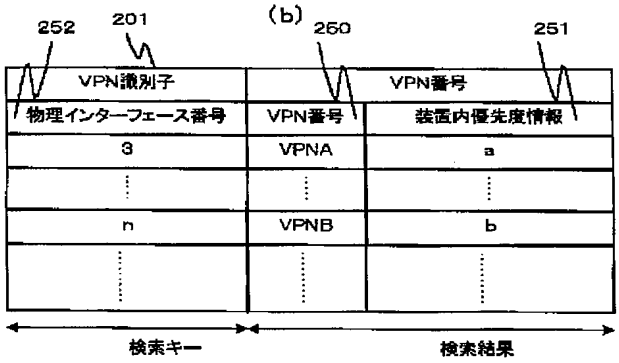
【図７】

図7

(a)

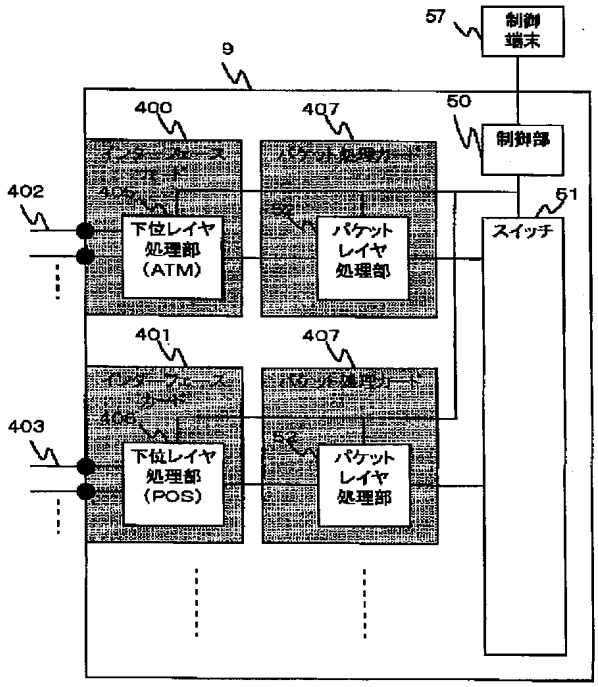


(b)



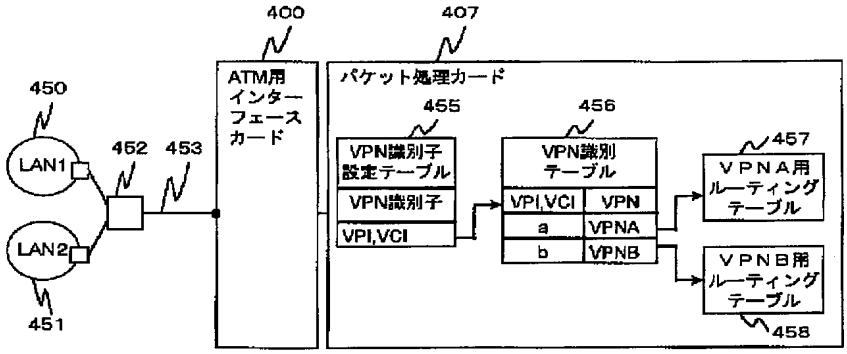
【図９】

図9



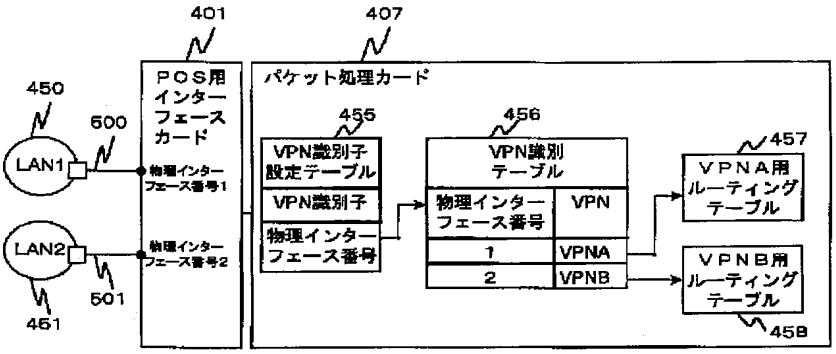
【図１０】

図10



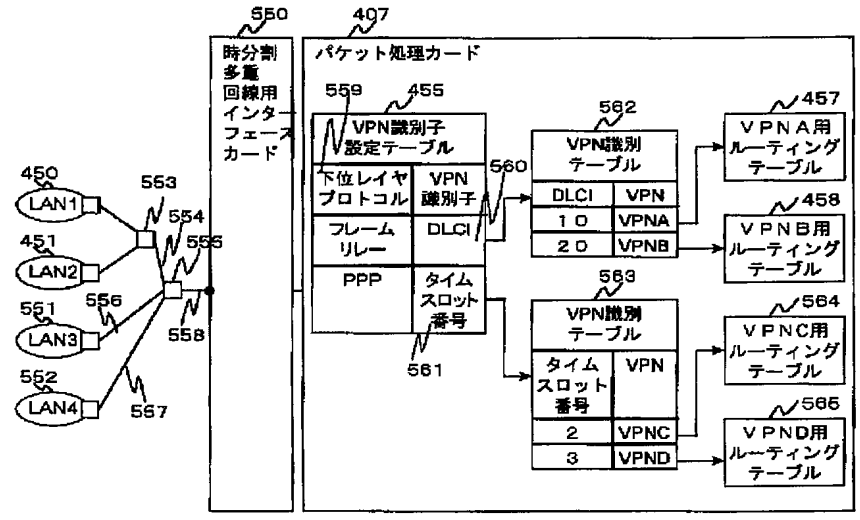
【図１１】

図11



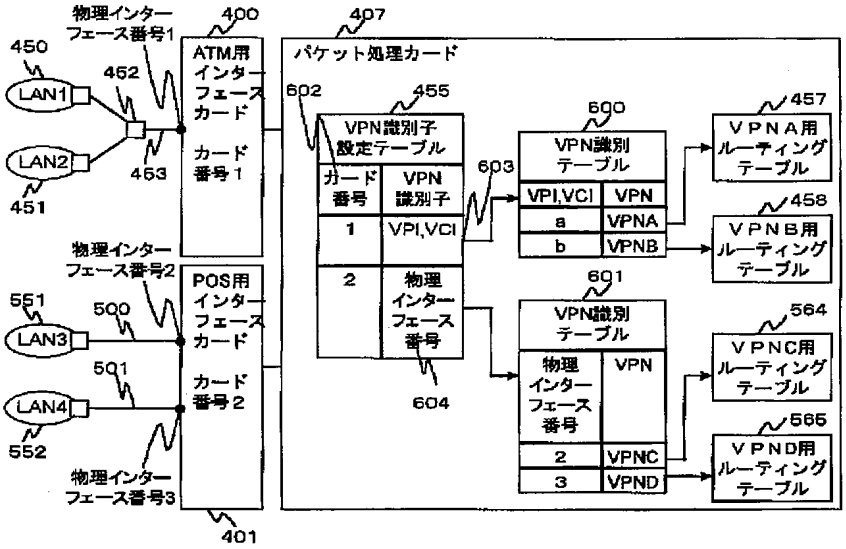
【図１２】

図12



【図１３】

図13



フロントページの続き

(72)発明者　須貝　和雄
神奈川県秦野市堀山下１番地　株式会社日立製作所エンタープライズサーバ事業部内

Ｆターム(参考)　5K030 GA04 HA08 HA09 HA10 HB14 HC01 HC14 HD03 KA05 LB05 LD17
5K033 AA04 CB08 DA06 DB12